CLAIMS

1. An arrangement for blocking of unwanted network traffic in open data and telecommunication networks, characterized by comprising:

a first level of blocking (350) in the form of a top level domain requiring registration for web sites (390) residing within the domain with respect to ordre public;

at least one top level domain server (16) for connection to the top level domain comprising or being connected to a domain name server (14) files and software, which assign a call, through computer (12), a network address (340) which associates to a correct application server (380) when the user of computer (12) has been identified;

database means (18), connected to the top level domain server (16) for registration and approval of a services provider (19) residing within the top level domain;

means connected to or comprised in the top level domain server (16) for identification of a calling parties identity (310) during login to the top level domain;

means connected to or comprised in the top level domain server (16) for blocking (330) an unidentified calling party; and

whereby registration of those connected to the domain and the identification of a calling party prevents a free connection and anonymity in computer networks through said top level domain server (16), which accomplishes a top level domain purged from unwanted network traffic.

2. An arrangement according to claim 1, characterized in that a second level of blocking (400) comprises micro debiting through a debiting server (20) during connection (410) to the top level domain by:

means for debiting of the top level domain via micro debiting;

2

means for accumulation of said micro debiting during every session a user is connected to said domain.

3. An arrangement according to claim 2, characterized in that the web address of the one connected (12) is stored for debiting in a database (18).

4. An arrangement according to claim 3, characterized by comprising:

means in the debiting server (20) for percentage partitions in at least two posts of accumulated micro debitings for every session during login, which posts are credited to at least one of the top level domain and a registered service provider.

5. A method relating to an arrangement for blocking of unwanted network traffic in open data and telecommunication networks, characterized by comprising the method steps of:

providing a first level of blocking (350) in the form of a top level domain requiring registration for web sites (390) residing within the domain with respect to ordre public;

connecting at least one top level domain server (16) for connection to the top level domain comprising or being connected to a domain name server (14) files and software, which assign a call, through computer (12), a network address (340) which associates to a correct application server (380) when the user of computer (12) has been identified;

connecting database means (18), connected to the top level domain server (16) for registration and approval of a services provider (19) residing within the top level domain;

identifying a calling parties identity (320) during login to the top level domain;

blocking (330) through means for such a purpose of an unidentified calling party; and

whereby registration of those connected to the domain and the identification of a calling party prevents a free connection and anonymity in computer networks through said top

level domain server (16), which accomplishes a top level domain purged from unwanted network traffic.

6. A method relating to an arrangement for blocking according to claim 5, characterized in that a second level of blocking (400) comprises micro debiting through a debiting server (20) during connection (410) to the top level domain by:

means for debiting of the top level domain via micro debiting;

means for accumulation of said micro debiting during every session a user is connected to said domain.

7. A method relating to an arrangement for blocking according to claim 6, characterized in that the web address of the one connected (12) is stored for debiting in a database (18).

8. A method relating to an arrangement for blocking according to claim 7, characterized by comprising means in the debiting server (20) for percentage partitions in at least two posts of accumulated micro debitings for every session during login, which posts are credited to at least one of the top level domain and a registered service provider.

9. An arrangement according to claim 2, characterized by comprising:

means in the debiting server (20) for percentage partitions in at least two posts of accumulated micro debitings for every session during login, which posts are credited to at least one of the top level domain and a registered service provider.

10. A method relating to an arrangement for blocking according to claim 6, characterized by comprising means in the debiting server (20) for percentage partitions in at least two posts of accumulated micro debitings for every session during login, which posts are credited to at least one of the top level domain and a registered service provider.

4